UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/559,414	04/26/2000	Greg Rosenberg	3974-4001	1221

7590 12/03/2003

William E Sekyi
Morgan & Finnegan LLP
345 Park Avenue
New York, NY 10154

EXAMINER	
VAUGHAN, MICHAEL R	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 12/03/2003

3

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/559,414	ROSENBERG, GREG	
	Examiner	Art Unit	
	Michael R Vaughan	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 April 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-45* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 April 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *2*.
4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Claims 1-45 have been examined and are pending.

Information Disclosure Statement

An initialed and dated copy of Applicant's IDS form 1449, Paper No. 2, is attached to the instant Office action.

Specification

Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

The abstract of the disclosure is objected to because the length of the abstract exceeds 150 words. Correction is required. See MPEP § 608.01(b).

Claim Rejections - 35 USC ' 112, second paragraph

Claim 29 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 29 mentions both a "second memory device" and a "third memory device" as being the same entity. Clarification and/or correction are required.

Claim Rejections - 35 USC ' 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-16, 24-29, 31-33, 36-40, and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Herzberg and Naor of Surf'N'Sign (here within Surf) in view of Ganesan (USP 5,535,276).

As per claim 1, 25, and 36 Surf teaches:

A method of signing and authenticating electronic documents comprising (pg. 1):

receiving at the local computer cluster a signing request transmitted from a first remote computer by a first user; identifying the signing request as one transmitted by the first user (pg. 6), and identifying a signature ready document to be signed (pg. 7);

retrieving at the local computer cluster the signature ready document to be signed (pg. 7);

signing the signature ready document on the local computer cluster using a complete private key to produce a signed document (pgs. 6-7).

Surf is silent in expressly disclosing:

retrieving at the local computer cluster a private key portion associated with the first user from the private key database generating a complete private key using the retrieved private key portion if the retrieved private key portion is not a complete private key; and

securely storing a plurality of private key portions associated with a plurality of users in a private key database on a local computer cluster.

Ganesan teaches:

securely storing a plurality of private key portions associated with a plurality of users in a private key database on a local computer cluster (column 8, lines 11-43 and column);

retrieving at the local computer cluster a private key portion associated with the first user (column 11, lines 29-31) from the private key database generating a complete private key using the retrieved private key portion if the retrieved private key portion is not a complete private key (column 12, lines 45-53). Ganesan teaches that it is advantageous for a trusted third party to maintain one portion of every user's RSA private key (column 3, lines 17-25). This forces the user to interact with a trusted third party, which provides practical advantages such as instant revocation.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Ganesan within the system of Surf because interacting with a trusted third party by allowing it to do the signing improves the overall security of the system to all parties involved. One skilled in the art would have been motivated to generate the claimed invention with a reasonable expectation of success.

As per claim 2, Surf teaches the private key portion is a complete private key (pg. 7).

As per claim 3, Surf teaches receiving signing identification credentials from the first user (pgs. 6-7). Surf fails to teach constructing a complete private key using the private key portion and the received signing identification credentials. Ganesan teaches constructing a complete private key using the private key portion and the received signing identification credentials (column 12, lines 45-65 and column 14, lines 10-40). The examiner supplies to same rationale for the motivation to incorporate the teachings of Ganesan within the system of Surf as recited in the rejection of claim 1. Surf teaches sending identification credentials to the server. Furthermore, it would have been obvious to one of ordinary skill in the art to generate the server side of the private key with identifying credentials because it associates the key with the intended user.

As per claim 4, Surf teaches the received signing request was transmitted from the first remote computer to the local computer cluster over the internet (pg.4).

As per claim 5, Surf teaches the received signing request was transmitted from the first remote computer to the local computer cluster over the world wide web using a hypertext transport protocol, and wherein the signing request was transmitted using a browser running on the remote computer (pg. 4).

As per claims 6 and 33, Surf teaches the retrieving at the local computer cluster the signature ready document is automatic (pgs 6-7).

As per claims 7 and 32, Surf teaches the retrieved signature ready document is a standard generalized markup language document (pg. 4).

As per claims 8, 26, and 37, Surf teaches storing the signature ready document in a first document database (pg. 6).

As per claims 9 and 31, Surf teaches prior to signing: receiving form data from the first remote computer; and modifying the retrieved signature ready document based on the received form data (pgs. 2-4).

As per claims 10 and 27, Surf teaches the first document database is located on the local cluster (pg. 6).

As per claim 11, Surf fails to teach the first document database is located on a secure second remote computer. Ganesan teaches the first document database is located on a secure second remote computer (see figure 2, element 140). Separating the responsibilities of entities protects the users from having to put all of the trust in one entity. Ganesan teaches a system whereby the duties of the secure environment are broken up among participating servers. Therefore, if the trust of one entity is found to be compromised then the whole system is not compromised. Only the information of entity needs to be recreated.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Ganesan within the system of Surf because divvying the trust among servers reduces the level of trust one must have with a particular server. One skilled in the art would have been motivated to generate the claimed invention with a reasonable expectation of success.

As per claims 12, 28, and 38, Surf teaches storing the signed document in a second document database (pg. 6).

As per claims 13 and 29, Surf teaches the second database is located on a secure second computer remote computer (pg. 6).

As per claim 14, Surf teaches the second database is located on the local computer cluster (pg. 6).

As per claims 15 and 39, Surf teaches associating at least one of the signature ready document and the signed document with a document owner (pg. 6-7).

As per claims 16 and 40, Surf teaches notifying at least one of document owner and the first user that a signature ready document or a signed document has been signed (pg. 6).

As per claim 24, Surf teaches a method of signing and authenticating electronic documents comprising:

running a browser on a first remote computer (pg. 6);

connecting to a local computer cluster via a computer network using the browser (pg. 6);

transmitting user identification information and document identification information to the local computer cluster (pgs. 6-7);

transmitting a signing request to the local computer cluster, the signing request requesting the local computer cluster to retrieve the identified document from a second remote computer (pgs. 6-7), but fails to teach to obtain a private encryption key associated with the identified user from a third remote computer, and to sign the retrieved document using the obtained private key on a fourth computer, wherein the first, second, third, and fourth remote computers can be the same computer or different computers. Ganesan teaches obtain a private encryption key associated with the identified user from a computer (column 11, lines 29-31), and to sign the retrieved document using the obtained private key (column 12, lines 45-65 and column 14, lines 10-40). Ganesan teaches that it is advantageous for a trusted third party to maintain one portion of every user's RSA private key (column 3, lines 17-25). This forces the user to interact with a trusted third party, which provides practical advantages such as instant revocation.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Ganesan within the system of Surf because interacting with a trusted third party by allowing it to do the signing improves the overall security of the system to all parties involved. One skilled in the art would have been motivated to generate the claimed invention with a reasonable expectation of success.

As per claim 44, Surf teaches the first user is a registered user (pg. 8).

Claims 17-21, 23, 30, 34, 35, 41, 42, 43, and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Surf and Ganesan as applied to claims 1 and 17 above, and further in view of Smithies et al (5,544,255).

As per claims 17, 18, 41, and 42, Surf teaches registering individuals as users, wherein registering includes: verifying and recording the identity of individuals registering (pg. 8). Surf fails to teach digitizing and recording handwritten signatures (which is an example of a biometric measurement) of individuals registering; associating passwords with the recorded digitized handwritten signatures and the recorded identities; and storing the recorded digitized handwritten signatures, and the recorded identities in an identity database, the identity database being accessible to the local computer cluster. Smithies et al teach digitizing and recording handwritten signatures of individuals registering (column 3, line 35—column 4, lines 58); associating passwords with the recorded digitized handwritten signatures and the recorded identities (column 17, lines 14-21); and storing the recorded digitized handwritten signatures, and the recorded identities in an identity database, the identity database being accessible to the local computer cluster (column 5, lines 5-12). The combined teachings of Surf and Ganesan rely on a trusted server to perform the authentication process to allow access to a resource such as a document. Ganesan teaches authenticating a user to a trusted server (column 8, lines 33-34). Smithies et al teach a method whereby a user can authenticate himself or herself to a remote computer system, thereby

allowing access to a particular electronic document (column 6, lines 29-44). Smithies et al teach a signature can be transmitted to a remote site for verification before allowing access to a computer system and that the computer system can verify a handwritten signature. Therefore, a handwritten signature is a way in which a computer system can grant authentication to a user who has registered.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Smithies et al within the combined system of Surf and Ganesan because the use of digital handwritten signatures is a way that a trusted server can viably authenticate a user. One skilled in the art would have been motivated to generate the claimed invention with a reasonable expectation of success.

As per claims 19 and 43, the Surf and Ganesan are silent in disclosing the biometric measurements can determine whether individuals have previously registered. Smithies et al teach using the biometric measurements to determine whether individuals have previously registered (column 18, lines 1-23). Smithies teaches that it is important to keep track of who has registered because only those that have registered can be granted access into the system. Therefore, it is obvious that the system must be able to distinguish new users from registered users. In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Smithies et al within the combined system of Surf and Ganesan because Surf teaches registering users it would be advantageous to keep track of the users that have registered so that the system can distinguish new users from registered users. One skilled in the art would have been motivated to generate the claimed invention with a reasonable expectation of success.

As per claims 20, Surf teaches the first user is a registered user (pg. 8).

As per claims 21 and 45, Surf teaches appending a signature to a document but does not teach a digitized signature. Smithies et al teach appending the first user's digitized signature to the signature ready document; making a hash of the signature ready document; and encrypting the hash of the signature read), document with the first user's private key (column 20, lines 23-64 and column 13, lines 36-56). The examiner supplies the same rationale for the motivation as recited in the rejection of claim 17 to incorporate the use of a digitized signature as means to authenticate. Smithies et al teach hashing the

signature and encrypting the hash with the user's key to further insure that the signed document cannot be altered or duplicated. Therefore, it would be advantageous to take these extra steps to insure the validity of a signed document.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Smithies et al within the combined system of Surf and Ganesan because one would want to protect a signed document from being altered or duplicated. One skilled in the art would have been motivated to generate the claimed invention with a reasonable expectation of success.

As per claim 23, Surf teaches receiving signing identification credentials from the first user (pgs. 6-7). Surf fails to teach generating the private key portions for individuals registering, wherein the private key portions can be used with signing identification credentials to construct complete private keys; associating the generated private key portions with the recorded identities of individuals registering storing private key portions in a private key database. Ganesan teaches generating the private key portions for individuals registering, wherein the private key portions can be used with signing identification credentials to construct complete private keys (column 12, lines 45-65 and column 14, lines 10-40); associating the generated private key portions with the recorded identities of individuals registering (column 14, lines 10-40); and storing private key portions in a private key database (column 8, lines 11-43 and column). The examiner supplies to same rationale for the motivation to incorporate the teachings of Ganesan within the system of Surf as recited in the rejection of claim 1. Surf teaches sending identification credentials to the server. Furthermore, it would have been obvious to one of ordinary skill in the art to generate the server side of the private key with identifying credentials because it associates the key with the intended user.

As per claim 30, Surf teaches the local computer cluster further comprises a second memory device having stored thereon an identity database (pgs. 6-8), the identity database including recorded user identities associated with signatures but is silent in disclosing user digitized handwritten signatures and passwords associated with the user identities. Smithies et al teach the identity database includes user digitized handwritten signatures and passwords associated with the user identities (column 17, lines

14-20). Smithies et al use this teaching in order to organize its users and their respective identifying information so that the system can correctly link and identify a user with his/her data as a way to authenticate. Surf stores the signed documents in a database with some identifying information but not to the extent that Smithies et al teach. It would be advantageous to the system of Surf to provide a more secure means to authenticate a person before the system allows a user to view a signed document. Smithies et al teachings provide such a means.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Smithies within the combined system of Surf and Ganesan because it would allow the system to have a more secure method of authentication. One skilled in the art would have been motivated to generate the claimed invention with a reasonable expectation of success.

As per claim 34, Surf fails to teach a registration computer connected to the local computer cluster. Surf teaches that registration is performed as signing occurs (pgs. 6-8). Smithies et al teach a registration computer connected to the local computer cluster (column 17, lines 5-43). Smithies et al use this teaching in order to organize its users and their respective identifying information so that the system can correctly link and identify a user with his/her data as a way to authenticate. Smithies et al use the registration computer before a user is allows access to the database services. This increases the overall security of the system. Therefore, it would be advantageous to use a registration computer to prevent unauthorized user from gaining access to the system.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Smithies within the combined system of Surf and Ganesan because it would allow the system to prevent users who have not yet registered from using the system's resources. One skilled in the art would have been motivated to generate the claimed invention with a reasonable expectation of success.

As per claim 35 Surf teaches registering individuals as users, wherein registering includes: verifying and recording the identity of individuals registering (pg. 8). Surf fails to teach digitizing and recording handwritten signatures (which is an example of a biometric measurement) of individuals registering; associating passwords with the recorded digitized handwritten signatures and the recorded

identities; and storing the recorded digitized handwritten signatures, and the recorded identities in an identity database, the identity database being accessible to the local computer cluster. Smithies et al teach digitizing and recording handwritten signatures of individuals registering (column 3, line 35—column 4, lines 58); associating passwords with the recorded digitized handwritten signatures and the recorded identities (column 17, lines 14-21); and storing the recorded digitized handwritten signatures, and the recorded identities in an identity database, the identity database being accessible to the local computer cluster (column 5, lines 5-12). The combined teachings of Surf and Ganesan rely on a trusted server to perform the authentication process to allow access to a resource such as a document. Ganesan teaches authenticating a user to a trusted server (column 8, lines 33-34). Smithies et al teach a method whereby a user can authenticate himself or herself to a remote computer system, thereby allowing access to a particular electronic document (column 6, lines 29-44). Smithies et al teach a signature can be transmitted to a remote site for verification before allowing access to a computer system and that the computer system can verify a handwritten signature. Therefore, a handwritten signature is a way in which a computer system can grant authentication to a user who has registered.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Smithies et al within the combined system of Surf and Ganesan because digital handwritten signature are a way that a trusted server can viably authenticate a user. One skilled in the art would have been motivated to generate the claimed invention with a reasonable expectation of success.

Claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over Surf, Ganesan, Smithies as applied to claims 1 and 17 above, and further in view of Shin (USP 6,351,634 B1).

As per claim 22, Surf is silent in disclosing:

associating and storing a secret set of recognition graphics with the passwords in the identity database;

displaying a plurality of recognition graphics, including recognition graphics from the secret set, on the first remote computer;

requesting the first user to select graphics included in the secret set using a non-keyboard selecting device attached to the first remote computer;

receiving a message from the first remote computer identifying the selected graphics;

authorizing access to the local computer cluster if the selected graphics are included in the secret set.

Shin discloses:

associating and storing a secret set of recognition graphics with the passwords in the identity database (column 1, line 60—column 3, line 21);

displaying a plurality of recognition graphics, including recognition graphics from the secret set, on the first remote computer (column 1, line 60—column 3, line 21);

requesting the first user to select graphics included in the secret set using a non-keyboard selecting device attached to the first remote computer (column 1, line 60—column 3, line 21);

receiving a message from the first remote computer identifying the selected graphics (column 1, line 60—column 3, line 21);

authorizing access to the local computer cluster if the selected graphics are included in the secret set (column 1, line 60—column 3, line 21).

Shin teaches that his method of authentication is better than methods using just keypad data entries. He suggests it is harder for someone to gain knowledge of a secret symbol than gaining knowledge of keypad alphanumeric passwords. Therefore, it would be advantageous to the overall security of the system is authentication was assisted by determining secret symbols as opposed to just alphanumeric passwords.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Shin within the combined system of Surf and Ganesan and Smithies et al because it would allow the system to have a more secure method of authentication. One

skilled in the art would have been motivated to generate the claimed invention with a reasonable expectation of success.

Remarks

No claim is allowed.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patents :

5,737,419	Ganesan
6,401,206	Khan et al.

Foreign Patents :

WO 9,905,818	Cocks

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael R Vaughan whose telephone number is 703-305-0354. The examiner can normally be reached on M-F 7:30-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

MV
Michael R Vaughan
Examiner
Art Unit 2131

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100